2010/35 Inland

https://shop.jungle.world/artikel/2010/35/schreib-mal-wieder

Der E-Postbrief und die Probleme mit der Sicherheit

Schreib mal wieder!

Von **claire sinn**

Briefgeheimnis, Datenschutz? Der »E-Postbrief« der Deutschen Post ist zwar nach seinem analogen Vorbild benannt. Wer ihn oder ein Konkurrenzprodukt nutzt, kann sich jedoch keinesfalls auf eine sichere Kommunikation verlassen.

Man stelle sich vor: Jemand gründet einen Internetdienst, der die Zustellung von Telegrammen simuliert. Empfänger, die im Besitz einer E-Mail-Adresse sind, bekommen die Telegramme auf elektronischem Weg zugestellt, angereichert mit den typischen Insignien wie »Zahlungsaufforderung STOP zahlbar bis ... «. Um das Konzept noch umständlicher und überflüssiger zu machen, wird Verweigerern der neuen Medien die Nachricht von einem Telegrammboten überreicht. Das mutet wie eine bierselige, zum Scheitern verurteilte Dotcom-Idee an. Dennoch ist der Einfall nun ganz ähnlich verwirklicht worden.
Seit kurzem gibt es den »E-Postbrief«. Die Bezeichnung klingt wie ein Markenname aus dem Paralleluniversum deutscher Nationalisten, die bekanntlich eine Abneigung gegen Anglizismen haben. Der »E-Postbrief« wird aber von der Deutschen Post AG, einem Global Player in Sachen Transport und Logistik, angeboten. Zunächst hatte sich eine Arbeitsgruppe des Innenministeriums damit beschäftigt, eine Prozedur für den Versand rechtsverbindlicher E-Mails zu entwickeln. Zahlreiche Internet-Provider, die Deutsche Telekom und die Post arbeiteten anschließend etliche Jahre lang gemeinsam an der Idee: Ziel des Verfahrens ist die zweifelsfreie Identifikation von Sender und Empfänger einer E-Mail.

Bis zum Ende dieses Jahres soll nun ein Bürgerportalgesetz verabschiedet werden, das diese Art der elektronischen Briefkommunikation vor allem für den Geschäfts- und Behördenverkehr regelt. Aus Sorge um das eigene herkömmliche Briefgeschäft zog sich die Post im Laufe der Entwicklung zurück und bietet nun den »E-Postbrief« an. Web.de, GMX und die Deutsche Telekom wollen zum Jahreswechsel das Konkurrenzprodukt »De-Mail« auf den Markt bringen. Jeder Nutzer des »E-Postbriefs« soll nach erfolgreicher Anmeldung in der Lage sein, Empfängern ein rechtsverbindliches Schreiben zukommen zu lassen. Nimmt der Empfänger nicht am digitalen Verfahren teil, dann wird der Brief ausgedruckt und ihm auf herkömmlichem Weg zugestellt. Die Allgemeinen Geschäftsbedingungen der Post nehmen den Nutzer in die Pflicht, für die Datensicherheit aufzukommen.
»De-Mail« hingegen behält es sich vor, die Korrespondenz selbst auf Viren und Spam zu überprüfen. Die Anbieter erklären ausdrücklich, dass keine gesicherte Ende-zu-Ende-

Kommunikation stattfindet, der Brief also nicht unangetastet und vertraulich übermittelt wird. Die Sicherheit ist Sache des Anbieters, es ist zu befürchten, dass »De-Mail« dieses geplante Vorgehen als Beweis der eigenen Vertrauenswürdigkeit vermarkten wird. Vollkommen unklar ist, was passiert, wenn Nutzer ihrerseits ein Verschlüsselungsverfahren verwenden, an dem der Viren- und Spamfilter von »De-Mail« scheitert. Aber auch der »E-Postbrief« sieht eine Speicherung der Mails vor, selbst wenn der Kunde seine Mail längst löschen möchte.
Warum staatliche Behörden und Unternehmen die Verbreitung des elektronischen Einschreibens vorantreiben, liegt auf der Hand. Immerhin geht es um einen Betrag zwischen 40 und 70 Millionen Euro, der jährlich eingespart werden könnte. Aber auch gewöhnliche Nutzer sind anscheinend ganz wild darauf, den von Staat und Unternehmen erfassten Daten zur physischen Existenz einen digitalen Avatar zur Seite zu stellen. Die Testphase von »De-Mail« in Friedrichshafen stieß bei den Anwendern überwiegend auf Begeisterung, Bedenken werden anscheinend dem unbändigen Always-Online-Wunsch untergeordnet.

Da etwa beim Schriftwechsel mit Behörden das Gegenseitigkeitsprinzip gilt, ist jeder, der einmal die Dienste zum Versand des »E-Postbriefs« in Anspruch genommen hat, auch zum Empfang auf diesem Wege verpflichtet. Das kann unangenehme Konsequenzen haben, zum Beispiel wenn es darum geht, Fristen einzuhalten. Gelten herkömmliche Briefe drei Werktage nach Aufgabe als zugestellt, kennt »De-Mail« Entwürfen zufolge kein Wochenende. Gänzlich unklar ist die Regelung beim Hybrid-Verfahren des »E-Postbriefs«. Ein am Donnerstag digital aufgegebener Brief wird kaum am Sonntag im Briefkasten liegen.
»Wir bringen das Briefgeheimnis ins Internet.« Der Slogan der Post ist falsch. Den Allgemeinen Geschäftsbedingungen für Privatkunden des »E-Postbriefs« zufolge unterliegt dieser lediglich den Vorgaben der Telekommunikations-Überwachungsverordnung (TKÜV) und des Telekommunikationsgesetzes (TKG), aber nicht dem Briefgeheimnis. Dieses wird in Artikel 10 des Grundgesetzes garantiert. Der Paragraph 113 des TKG dagegen gewährt Ermittlungsbehörden umfangreichen Zugriff auf elektronische Korrespondenz.
Neben diesen Unannehmlichkeiten hat das Verfahren das Potential, einen Paradigmenwechsel in der E-Mail-Kommunikation herbeizuführen. Bisher waren alle Sender und Empfänger von E-Mails mehr oder minder gleichberechtigte Partner. Nun könnte jede Kommunikation, die nicht den Segen von »De-Mail« oder des »E-Postbriefs« hat, zu minderwertiger Bulk-Mail verkommen. Zwar steht es grundsätzlich allen Institutionen frei, sich bei »De-Mail« zu akkreditieren. Doch die vom Bundesamt für die Sicherheit in der Informationstechnik ausgearbeiteten, 42 Punkte umfassenden Vorgaben sind für kleine Unternehmen und Vereine kaum einzuhalten.

Die Möglichkeit, Kommunikationspartner im Internet zweifelsfrei zu identifizieren, besteht seit fast zwei Jahrzehnten (Jungle World 10/05). Die 1991 von Philip Zimmerman entwickelte Software »Pretty Good Privacy« (PGP) gewährleistet nicht nur die Vertraulichkeit in der E-Mail-Korrespondenz, sondern auch die Authentizität des Absenders. PGP und seine Derivate wie der Gnu Privacy Guard fanden jedoch nie größere Verbreitung. Die Gründe für das Scheitern sind zahlreich. Bis heute darf kryptografische Software in vielen Ländern nicht oder nur in stark eingeschränkter Funktion verwendet werden. Auch setzt Open-PGP-Software ein gewisse Bereitschaft des Nutzers voraus, sich mit der Materie auseinandersetzen. Doch Kriminalisierung und technische Hürden sind nicht die einzigen Gründe für die geringe Akzeptanz. Open-PGP verfolgt einen puristischen Ansatz, bei dem es nur darum geht, auf dem Weg der Nachricht zwischen den Kommunikationspartnern jederzeit ein Verschlüsselung zu garantieren. Entwicklungen hin zu einer halbttransparenten Verschlüsselung und Signierung waren für die Verfechter von Open-PGP-Software unbefriedigend.

Zweifellos ist der Wunsch nach einer Welt ohne Spam berechtigt. Dass der »E-Postbrief« dieses Versprechen einlösen wird, ist unwahrscheinlich. In einer weiteren Passage der Geschäftsbedingungen heißt es: »Falls der Veröffentlichung der Daten im Adressverzeichnis zugestimmt wurde, können diese Angaben von der Deutschen Post AG an andere registrierte Geschäftskunden/Versender auf Anfrage auch beauskunftet werden.« Geschäftsleute, die mit Adressen und anderen personenbezogenen Daten handeln, werden so eingeladen, die Informationen aus dem Adressverzeichnis gewinnbringend zu verhökern. Auf diesem Weg könnte sich das Modell selbst diskreditieren, wenn demnächst Online-Apotheken und andere Anbieter vollkommen ordnungsgemäß authentifiziert ihre Produktinformationen zu Potenzmitteln per »E-Postbrief« verschicken.